

FORM PTO-1449 U.S. Department of
Commerce (Rev. 4/92) Patent and Trademark

ATTY. DOCKET NO.

SERIAL NO.

500.42884X00

10/608,209

APPLICANT

T. ENDO, et al

FILING DATE

June 30, 2003

GROUP

2121

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use several sheets if necessary)

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT	
						YES	NO
CN	0 3 0 0 1 3 6 2	1/2003	PCT				

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

CN	B. Boer "A DPA Attack against the Modular Reduction within a CRT Implementation of RSA", Cryptographic Hardware and Embedded Systems, Ches 2002, 4 th International Workshop, Revised Papers (Springer Verlag, Lecture Notes in Computer Science, vol. 2523), July 15, 2002, pp. 228-243.
CN	J. Dhem et al, "A Practical Implementation of the Timing Attack", Smart Card Research and Applications, Third International Conference, Cardis '98 (Springer Verlag, Lectures Notes in Computer Science vol. 1820, Sep. 16, 1998, pages 1-18.

EXAMINER /Chuong Ngo/

DATE CONSIDERED

07/22/2006

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(Form PTO-1449 [6-4])